The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED:

10/10/2013

10/11/2013 - ***Updated***

SUBJECT:

Spear Phishing Emails Targeting State Executives

Original Description:

ITS was notified by a trusted third party about spear phishing emails targeting State Executives, including Fusion Center Directors. These emails contain a virus as an attachment and a spoofed sender address.

October 11 - Updated Description:

ITS has received reports that the malware delivered via the phishing e-mail has been observed downloading CryptoLocker malware. CryptoLocker is ransomware which seeks out and encrypts documents on the infected machine and any connected shares or drives. The encrypted files are held ransom for a fee. If the fee is not paid within a specific timeframe, typically seventy-two hours, the encrypted files will be deleted. Decryption is only feasibly possible given the purchase of the key. However, open source intelligence suggests paying the fee does not always result in the restoration of files.

It should be noted that once the victim is infected, the CryptoLocker malware may not be downloaded immediately. It has been reported that CryptoLocker has been downloaded as long as twenty-four hours following the initial infection. Because of this, it is important that infected systems be identified as quickly as possible and remediated immediately.

Original Indicators:

The attachment is currently being detected by all of the major AV products with various names including ZBot, Cutwail and Kazy. If the malware is installed, it will attempt to connect to warehousesale[dot]com[dot]my on port 443/TCP.

Sample Email Indicators:

Subject: “Annual Form - Authorization to Use Privately Owned Vehicle on State Business”

Attachment: Attachments follow the naming convention of “Form_[Varying Digits and Numbers].zip. For example: Form_nfcausa.org.zip, Form_20130810.exe, Form_f4f43454.com.zip.

Spoofed Sender: “fraud@aexp.com” “Dewayne@nfcausa.org”

Sender IP: 209.143.144.3

Sender Host: mail.netsential.com

October 11 - Updated Indicators - CryptoLocker:

Registry:

HKCU\Software\CryptoLocker

HKCU\Software\CryptoLocker\Files (This key reportedly contains a list of encrypted files)

HKCU\Software\Microsoft\Windows\CurrentVersion\Run CryptoLocker = <Reference to file location>

File System:

Windows Vista and later

C:\Users\<username>\AppData\Roaming\{CLSID}.exe

Windows XP and before

C:\Documents and Settings\<username>\Application Data\{CLSID}.exe

Original Recommendations:

The following actions should be taken:

* Search all available logs and identify any traffic destined to the above indicators.

* Search email inbox for message with the reported subject line, and delete those messages.

* For any mailboxes that received the messages described, investigate with the end-user about whether they downloaded attachments or followed the links within the email.

* Since most of these emails are originating from spoofed email accounts, educate your users on checking the senders of the e-mails and verify the legitimacy of the sender.
* Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
* Remind users to never click on links in emails, even from trusted sources.

October 11 - Updated Recommendations:

- ***If infected with CryptoLocker, remediate the infection via antivirus. Following the remediation, restore any encrypted files from backup or system restore points and volume shadow copies.***

References:

http://tools.cisco.com/security/center/viewAlert.x?alertId=31177

http://blog.mxlab.eu/2013/10/08/email-annual-form-authorization-to-use-privately-owned-vehicle-on-state-business-contains-new-trojan-variant/